ASA 7.x Manually Install third Party Vendor Certificates for use with WebVPN Configuration 예

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 구성 1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다. 2단계. RSA 키 쌍 생성 3단계. 신뢰 지점 생성 4단계. 인증서 등록 생성 5단계. 신뢰 지점 인증 6단계. 인증서 설치 7단계. 새로 설치된 인증서를 사용하도록 WebVPN을 구성합니다. 다음을 확인합니다. ASA에서 자체 서명 인증서 교체 설치된 인증서 보기 웹 브라우저를 사용하여 WebVPN에 설치된 인증서 확인 SSL 인증서 갱신 단계 명령 문제 해결 관련 정보

소개

이 컨피그레이션 예에서는 WebVPN과 함께 사용할 수 있도록 ASA에 서드파티 벤더 디지털 인증서 를 수동으로 설치하는 방법에 대해 설명합니다. 이 예에서는 Verisign 평가판 인증서가 사용됩니다. 각 단계에는 ASDM 애플리케이션 절차 및 CLI 예가 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서를 사용하려면 인증서 등록을 위해 CA(인증 기관)에 액세스할 수 있어야 합니다. 지원되는 타사 CA 공급업체는 Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, VeriSign입니다.

사용되는 구성 요소

이 문서에서는 소프트웨어 버전 7.2(1) 및 ASDM 버전 5.2(1)를 실행하는 ASA 5510을 사용합니다. 그러나 이 문서의 절차는 호환되는 모든 ASDM 버전과 함께 7.x를 실행하는 모든 ASA 어플라이언 스에서 작동합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

구성

PIX/ASA에 타사 공급업체 디지털 인증서를 설치하려면 다음 단계를 완료하십시오.

- 1. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.
- 2. <u>RSA 키 쌍을 생성합니다</u>.
- 3. <u>신뢰 지점을 만듭니다</u>.
- 4. <u>인증서 등록을 생성합니다</u>.
- 5. 신뢰 지점을 인증합니다.
- 6. 인증서를 설치합니다.
- 7. <u>새로 설치된 인증서를 사용하도록 WebVPN을 구성합니다</u>.

1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.

- 1. 구성을 클릭한 다음 속성을 클릭합니다.
- 2. Device Administration(디바이스 관리)을 확장하고 Clock(시계)을 선택합니다.
- 3. 나열된 정보가 정확한지 확인합니다.올바른 인증서 검증이 이루어지려면 날짜, 시간 및 표준 시간대 값이 정확해야 합니다



명령줄 예

ciscoasa
ciscoasa# show clock
11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

2단계. RSA 키 쌍 생성

생성된 RSA 공개 키는 ASA의 ID 정보와 결합하여 PKCS#10 인증서 요청을 생성합니다. 키 쌍을 만들 신뢰 지점을 사용하여 키 이름을 명확하게 식별해야 합니다.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Properties(속성)를 클릭합니다.
- 2. Certificate(**인증서**)를 확장하고 Key Pair(**키 쌍)를** 선택합니다.
- 3. Add(추가)를 클릭합니다

as .	E- Certificate		
65	Authentication		
NAT	Enrolment	Key Pair Name Usage Modulus Size	Add
	- Rey Pair		1
VDN	- An Manage Certificates		Show Details
	E- 🙀 Trustpoint		
A	- Sonfiguration		Delete
	- Export	🚺 Add Key Pair	
CSD Manager	- Import		1
	E B Device Access	C the defending on the	Refresh
25	E-38 Device Administration	Name: Use default key name	
Routing	E B DHC Services	G humaniting had	
0	E-ADNS 15	 Imv.vensign.xey] 	
68	High Availability and Scal		
Global Objects	- Failover	Size: 1024	
	- K Fragment		
5	-12 History Metrics	Usage: 🕫 General Purpose C Special	
Discounting 1	HTTP.HTTPS		
Properties	E-R IP Audit		
	🗄 🚺 Logging		
	Priority Queue	Generate Now Cancel Help	
	SUNRPC Server		
	TCP Options		
	- Timeouts		
	¥		

- 4. 키 이름을 입력하고 모듈러스 크기를 선택한 다음 사용 유형을 선택합니다. 참고: 권장 키 쌍 크기는 1024입니다.
- 5. Generate를 **클릭합니다**.생성한 키 쌍은 Key Pair Name(키 쌍 이름) 열에 나열되어야 합니다. **명령줄 예**

ciscoasa
ciscoasa# conf t
ciscoasa(config)# crypto key generate rsa label my.verisign.key modulus 1024
! Generates 1024 bit RSA key pair. "label" defines the name of the key pair. INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait ciscoasa(config)#

3단계. 신뢰 지점 생성

신뢰 지점은 ASA에서 사용할 CA(인증 기관)를 선언하는 데 필요합니다.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Properties(속성)를 클릭합니다.
- 2. Certificate(**인증서**)를 확장한 다음 Trustpoint(신뢰 지점)를 확장합니다.
- 3. Configuration(컨피그레이션)을 선택하고 Add(추가)를 클릭합니다

Configuration > Properties > Certificate > Trustpoint > Configuration						
Startup Wizard	Configur	ation				
🗊 🚮 AAA Setup	Conf	Configure a Certificate Authority (CA) as a trustpoint.				
	Com					
🔁 🐻 ARP						
Client Update				[]	[]	
E-E Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add	
Authentication						
Enrolment					Edit	
Import Certificate						
Key Pair						
Manage Certificates					Delete	
E-82 Trustpoint						
20 Contiguration		45			Request CRL	
Export						
import						
Device Access						

- 다음 값을 구성합니다.신뢰 지점 이름: 신뢰 지점 이름은 사용 용도와 관련이 있어야 합니다.
 (이 예에서는 my.verisign.trustpoint를 사용합니다.)키 쌍: 2단계에서 생성된 키 쌍을 선택합니다(my.verisign.key).
- 5. 수동 등록이 선택되었는지 확인합니다.
- 6. Certificate **Parameters를 클릭합니다**.Certificate Parameters 대화 상자가 나타납니다.
- 7. 편집을 클릭하고 이 테이블에 나열된 속성을 구성합니다.이러한 값을 구성하려면 속성 드롭다 운 목록에서 값을 선택하고 값을 입력한 다음 추가를 클릭합니다

		Common Name (CN)	webyph cisco.com
Attribute to be Added		Department (OU)	TSWEB
		Company Name (O)	Cisco Systems
ttribute: Select Attribute	Add >>	State (St)	North Carolina
		State (St)	US
alue:	Delete	Location (L)	Raleigh

- 8. 적절한 값을 추가한 후 **확인**을 클릭합니다.
- 9. Certificate Parameters(인증서 매개변수) 대화 상자의 Specify FQDN(FQDN 지정) 필드에 FQDN을 입력합니다.이 값은 CN(일반 이름)에 사용한 FQDN과 같아야 합니다

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh	
© Use FQDN of the device	
Specify FQDN webvpn.cisco.com	
O Use none	
E-mail:	
IP Address:	
Include device serial number	
OK Cancel Help	

10. **확인을 클릭합니다**.

.

- 11. 올바른 키 쌍이 선택되었는지 확인하고 수동 등록 사용 라디오 버튼을 클릭합니다.
- 12. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**

rustpoint Name: my.verisign.truspoint
Generate a self-signed certificate on enrollment
If this option is enabled, only Key Pair and Certificate Parameters can be specified.
Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced
Key Pair: my.verisign.key 💌 Show Details New Key Pair
Challenge Confirm Challenge
Password: Password:
Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.
Enroliment Mode
O Use manual enrolment
C Use automatic enrollment
Enrollment URL: http://
Retry Period: 1 minutes
Retry Count: Use 0 to indicate unlimited retries)

명령줄 예

ciscoasa
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint
! Creates the trustpoint.
ciscoasa(config-ca-trustpoint)# enrollment terminal
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>
Systems,C=US,St=North Carolina,L=Raleigh
<i>! Defines x.500 distinguished name.</i> ciscoasa(config-ca- trustpoint)# keypair my.verisign.key
<i>! Specifies key pair generated in <u>Step 3</u>.</i> ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

4단계. 인증서 등록 생성

ASDM 절차

- 1. Configuration(컨피그레이션)을 클릭한 다음 Properties(속성)를 클릭합니다.
- 2. Certificate(인증서)를 확장하고 Enrollment(등록)를 선택합니다.
- 3. <u>3단계</u>에서 생성된 신뢰 지점이 선택되었는지 확인하고 Enroll(등록)을 **클릭합니다**.인증서 등 록 요청(인증서 서명 요청이라고도 함)을 나열하는 대화 상자가 나타납니다

Enrollment Request	×
To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA.	
You will need to install the certificate after receiving it.	
Go to Configuration > Properties > Certificate > Import Certificate to do so.	
Certificate Request:	
hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN	
AQKBBQADgYOAMIGJAoGBALSYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm nsMFP7DeKPI0+PdthePBzngSgmlkmNYoMy6teicY9phTVgRcfyJH2dsBoL5ChlKY	
mAH40WUXbil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF	
$\verb+AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAdder and and an anti-adder and a statemeter and a statemeter address and a statemeter address addre$	
ghtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA	
gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3	
gEjVABVhB7Ni6N29710mDAbnPsOR3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0	
gomkG1011V2C3DA24BAM4SARqF@2CDdj0/33B1Q0GC-	
End - This line not part of the certificate request	
ок	

4. PKCS#10 등록 요청을 텍스트 파일로 복사한 다음 CSR을 해당 타사 공급업체에 제출합니다 .서드파티 벤더가 CSR을 수신한 후 설치를 위해 ID 인증서를 발급해야 합니다.

명령줄 예

장치 이름 1
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint
<pre>! Initiates CSR. This is the request to be ! submitted via web or email to the 3rd party vendor. % Start certificate enrollment % The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The</pre>
fully-qualified domain name in the certificate will be:

```
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes
! Displays the PKCS#10 enrollment request to the
terminal. ! You will need to copy this from the terminal
to a text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczE0
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
qwIDAOAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uol3yWCe OBzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request --- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

5단계. 신뢰 지점 인증

서드파티 벤더로부터 ID 인증서를 받은 후에는 이 단계를 진행할 수 있습니다.

- 1. 로컬 컴퓨터에 ID 인증서를 저장합니다.
- 2. base64로 인코딩된 인증서가 파일로 제공되지 않은 경우 base64 메시지를 복사하여 텍스트 파일에 붙여넣어야 합니다.
- 3. 확장명이 .cer인 파일의 이름을 바꿉니다.**참고:** 파일 이름이 .cer 확장명으로 변경되면 파일 아이콘이 인증서로 표시되어야 합니다.
- 4. 인증서 파일을 두 번 클릭합니다.Certificate 대화 상자가 나타납니다

ertificate	? ×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
 Ensures the identity of a remote computer Proves your identity to a remote computer 2.16.840.1.113733.1.7.21 	
	침

"*Windows*에 *이 인증서를 확인할 수 있는 정보가 충분하지 않은 경우* 이 절차를 진행하기 전에 타사 공급업체 루트 CA 또는 중간 CA 인증서를 받아야 합니다. 발급 루트 CA 또는 중간 CA 인증서를 얻으려면 타사 공급업체 또는 CA 관리자에게 문의하십시오.

- 5. Certificate **Path** 탭을 클릭합니다.
- 6. 발급된 ID 인증서 위에 있는 CA 인증서를 클릭하고 View Certificate(인증서 보기)를 클릭합니 Certificate

General Details Certification Path		
Certification path VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA Weise Webypn.cisco.com		
	View Certificate	
Certificate status:		
This certificate is OK.		
	ОК] _{중간 CA}

통간 CA 인증

서에 대한 자세한 정보가 나타납니다.**경고:** 이 단계에서 ID(장치) 인증서를 설치하지 마십시오 . 이 단계에서는 루트, 하위 루트 또는 CA 인증서만 추가됩니다. ID(디바이스) 인증서는 <u>6단계</u> 에 설치됩니다.

7. Details를 클릭합니다

Certificate	<u>? ×</u>
General Details Certification Path	1
Show: <a>All>	•
Field	Value
Serial number	v3 63 b1 a5 cd c5 9f 78 80 1d a0
Issuer	VeriSign Trial Secure Server Te
Valid to	Sunday, February 08, 2015 7: VeriSign Trial Secure Server Te
Public key	RSA (2048 Bits)
Ec	lit Properties Copy to File
	ОК

8. Copy **to File을 클릭합니다**.

.

9. 인증서 내보내기 마법사에서 다음을 클릭합니다.

10. Export File Format(파일 형식 내보내기) 대화 상자에서 Base-64 인코딩 X.509(.CER) 라디오 버튼을 클릭하고 Next(다음)를 클릭합니다

ificate Export Wizard	
Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
C Personal Information Exchange - PKCS #12 (.PFX)	
\square Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
<back next=""> C</back>	ance

11. CA 인증서를 저장할 파일 이름과 위치를 입력합니다. 12. Next(**다음**)를 클릭한 다음 Finish(마침)를 **클릭합니다**

.

-i cincace	e Export Wizard				
File to	Export	h a 61a	the commute		
Spe	ecify the name of ti	he file you wani	t to export		
File	ename:				
C	introotca				Browse
			< Back	Next >	Cancel

- 13. Export **Successful** 대화 상자에서 OK를 클릭합니다.
- 14. CA 인증서를 저장한 위치를 찾습니다.

.

15. 메모장과 같은 텍스트 편집기로 파일을 엽니다. (파일을 마우스 오른쪽 버튼으로 클릭하고 Send **To(보내기) > Notepad(메모장)를** 선택합니다.)base64로 인코딩된 메시지는 다음 이미 지의 인증서와 유사하게 표시되어야 합니다 File Edit Format View Help

----BEGIN CERTIFICATE---MIIFSj&CBDKgAwIBAgIQCECQ47aTdj6BtrI60/Vt6zANBgkghkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL ÉydGb3IqVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24qVHJpYWwqU2VjdXJlIFNl cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTk1OVowgZ4x CZAJB9NVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q2lzY28qU3lzdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BgNVBAsUMVRlcm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBWIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnhloweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52zXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9TvljTZWN1cmUtyWlhLnZlcmlzaWduLmNvbS9TvljUcmlhbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAWIaBBRLa7kolgYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTgIorIClawwwx+RHCcTqIrlzf0VfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvl×zŹji0J51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja idT1FmBvf02qaZS6S40= ----END CERTIFICATE-----

- 16. ASDM에서 Configuration(컨피그레이션)을 클릭한 다음 Properties(속성)를 클릭합니다.
- 17. Certificate(인증서)를 확장하고 Authentication(인증)을 선택합니다.
- 18. Enter the certificate text in 16진수 또는 base64 format 라디오 버튼을 클릭합니다.
- 19. 텍스트 편집기에서 base64 형식의 CA 인증서를 텍스트 영역에 붙여넣습니다.
- 20. Authenticate를 클릭합니다

Configuration > Properties > C	ertificate > Authentication					
Startup Wizard	Authentication					
AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated wi trustpoint and installed on the device.					
Client Update	Trustpoint Name: wy.verisign.truspo Verial Edit New					
Authentication	Fingerprint (optional):					
- Si Import Certificate - Si Key Pair	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.					
Annage Certificates	C Import from a file: Browse					
Export Mimport	Enter the certificate text in hexadecimal or base64 format: A1UE AvMoVmV/vaV/bb724aV/blav/MovmU2V/dXUENice7ic68U7VN0E bdp3					
⊕-∰ Device Administration ⊕-∰ DHCP Services ⊕-∰ DNS	ECCol67bggLewTagTia9h3MwDQYJKoZhvcNAQEFBQADgYEASz5v8s3/ Kqt234YROiL51ZS111oUZ2MANp2H4biw4ltfsG5snDDiwSRmiH3B/WSU6E Ai9TXvRicD5q0mB+nvK9tB2aBzOiaiHSiWzAJeQiuqA+Q93New+peui4Ahc					
High Availability and Scal	n&KK/+1Yv61w3+7g6ukFMARVBNg=					
History Metrics	Authentication Successful					
P Audit Logging Priority Queue SSL SSL	The trustpoint my.verisign.truspoint has been authenticated.					
TCP Options Timeouts URL Filtering	ОК					

21. **확인을 클릭합니다**. **명령줄 예**

IF.

CISCUASA
ciscoasa(config)# crypto ca authenticate
my.verisign.trustpoint
! Initiates the prompt to paste in the base64 CA root !
or intermediate certificate. Enter the base 64 encoded
CA certificate. End with the word "quit" on a line by
itselfBEGIN CERTIFICATE
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
${\tt jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw}$
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
Alvimcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZ1cmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD

QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
${\tt DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6}$
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
nvnFAQCVMDIWMAYIKWYBBQUHAGEWJGNUGHBZU18VG3G3LnZICMIZAWGU
CHMVdGvzdGnnLzAOBGNvHQ8BAI8EBAMCAQ1WEQ1J11Z1A1D4QGEBBAQD
AJUIAD~OWDDD~TofDIDE73Co/cobewarcccowwiCDccvvDVD0;DTCcwtCo
ATOUDY WEBAILTOOB 4 DF 255 D/ QODENY IGCCERW JCBS Y DVROJE IGAILON
MIGHIQSWCQIDVQQGEW0V0ZEAMBUGAIDECHMOVIIVYAVNDZZ4SIEIUIY4X
MDAUBYNV BACTIOZyci BUZYNOIFRI coByc?WzIF9ubHkuICBObyBbc3N1 cmFuY2Wz
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv
b30g00GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY21
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNg=
END CERTIFICATE
quit
! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
vaevovab /ICC5e3b Idde2C42 U813eI43 Do you accept this
certificate? [yes/no]: yes 'l'rustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non sell-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)#

6단계. 인증서 설치

ASDM 절차

.

타사 공급업체에서 제공하는 ID 인증서를 사용하여 다음 단계를 수행합니다.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Properties(속성)를 클릭합니다.
- 2. Certificate(인증서)를 확장한 다음 Import Certificate(인증서 가져오기)를 선택합니다.
- 3. Enter **the certificate text in 16진수 또는 base64 format** 라디오 버튼을 클릭하고 base64 ID 인 증서를 텍스트 필드에 붙여넣습니다

Configuration > Properties > C	ertificate > Import Certificate				
Startup Wizard	Import Certificate				
🕀 🚮 AAA Setup	Install an identity certificate that was received from a Certificate Authority (CA) in response to a manual				
- 🗔 Anti-Spoofing	encode a contract of the second				
🕀 🐻 ARP	en onnen request.				
🕀 🐼 Certificate	Trustpoint Name: my.verisign.fruspo Edit New				
- Authentication					
- Enrolment	Certificate Text				
Import Certificate	Characterize Bin				
Key Pair	Crowse				
Manage Certificates					
- A Trustpoint	 Enter the certificate text in hexadecimal or base64 format: 				
Configuration					
	u9BSOJsprEsHiyEFGDAmFiRodHRwOl8vbG9nby52ZXJpc2lnbi5jb20vdnNs MS5naWV/wDQYJKoZlhvcNAQEFBQADggEBAk/htvw5KFCgkwWXVdjjAr\ xutKsi5iP0c/EGCRCqaXe5xS+x9npPLsDNm8qTPAGRv4by2tj5UskQpcUQg; tFkFFSFbleCK/hin6MaMb40z6kiFlzpVUmtdJDoU3B00U/vm+tg02eTWdzrWE, 0YVwM3kDQAO6EbArtUoAxovDbJucdxb6ZVTtyevMcgzCKXMHEVxa5/P) ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4ufcGgGZD8tVGx26b5OWTz8KC				
- A Import					
Device Access					
Device Administration					
B-B DHCP Services					
High Auglahith and Cast	8EvHm3grdbDZP+ISMotVVYE+CgfKpZb+CPAqH2Cdpz2aJij,IN6CS6NM=				
Fallower	END CERTIFICATE				
Fragment					
- History Metrics					
HTTPHTTPS	📬 Information 🔀				
P Audit					
E-1 Logaing					
- Priority Queue	Certificate import succeeded.				
SSL .					
SUNRPC Server					
- 🔂 TCP Options					
Timeouts	OK				
URL Filtering					
⊕-m, MCCb					

4. Import(가져오기)를 클릭한 다음 OK(확인)를 클릭합니다. 명령줄 예

ciscoasa
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate
! Initiates prompt to paste the base64 identity certificate ! provided by the 3rd party vendor. % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itselfBEGIN
CERTIFICATE
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
${\tt yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw}$
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJ1IFN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G
AluebxQH
UmFsZWlnaDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECxQF
VFNXRUIX

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9ker2jQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxS1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc21nbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9T12tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
END CERTIFICATE
quit
INFO: Certificate successfully imported
ciscoasa(config)#

7단계. 새로 설치된 인증서를 사용하도록 WebVPN을 구성합니다.

- 1. Configuration(**구성)**을 클릭하고 **Properties(속성**)를 클릭한 다음 SSL을 선택합니다.
- 2. Trustpoints(신뢰 지점) 영역에서 WebVPN 세션을 종료하는 데 사용할 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스를 사용합니다.
- 3. Edit를 **클릭합니다**.Edit SSL Trustpoint 대화 상자가 나타납니다

Configuration > Properties > S	SL .
Startup Wizard	SSL
🕀 🚽 🖬 AAA Setup	Configure SSI parameters. These parameters affect both ASDM and Meh//EN access
- 3 Anti-Spoofing	Configure SSL parameters, mese parameters affect our ASDM and WebYPH access.
12-103 ARP	Server SSL Version: Any Client SSL Version: Any
	Encryption
	Electronic Contraction of Contractio
🕀 🔂 Certificate	Available Algorithms Add >> Active Algorithms Move Up
E Device Access	30ES-SHA1
1 Device Administration	The Edit SSL Trustmoint
E BHCP Services	
🕀 👼 DNS	Specify an enrolled trustpoint to be used for SSL authentication on the outside interface. To enroll a trustpoint
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.
- Failover	
Fragment	
-22 History Metrics	
HTTP/HTTPS	Interface: outside
P Audit	
Logging	Enroled Trustpoint: my.verisign.trustp
Priority Queue	
SUNKPC Server	
TCP Options	OK Cancei nep
UNL LIEL Electron	
H A WECE	Trustpoints
W VVCCP	Specify which enrolled trustopints, if any should be used for SSI authentication on each interface. The fallback
	trustopint will be used on interfaces not associated with a trustopint of their own.
	Fallback Trustroint
	Interface Trustpoint Edit
	management
	a diske mu verision trustraint
	a de la deservación d
I I	

- 4. Enrolled Trustpoint(등록된 신뢰 지점) 드롭다운 목록에서 <u>3단계</u>에서 생성한 신뢰 지점을 선택 합니다.
- 5. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

이제 지정된 인터페이스에서 종료되는 모든 WebVPN 세션에 새 인증서를 사용해야 합니다. 성공적 인 설치를 확인하는 방법은 이 문서의 확인 섹션을 참조하십시오.

명령줄 예

Ciscoasa ciscoasa(config)#ssl trust-point my.verisign.trustpoint outside ! Specifies the trustpoint that will supply the SSL ! certificate for the defined interface. ciscoasa(config)#write memory Building configuration... Cryptochecksum: 694687al f75042af ccc6addf 34d2cb08 8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)# ! Save configuration.

다음을 확인합니다.

이 섹션에서는 서드파티 벤더 인증서 설치가 성공했는지 확인하는 방법에 대해 설명합니다.

ASA에서 자체 서명 인증서 교체

이 섹션에서는 ASA에서 설치된 자체 서명 인증서를 교체하는 방법에 대해 설명합니다.

- 1. Verisign에 인증서 서명 요청을 발행합니다.Verisign에서 요청한 인증서를 받은 후에는 동일한 신뢰 지점 아래에 직접 설치할 수 있습니다.
- 2. 다음 명령을 입력합니다. crypto ca enroll verisign질문에 답하라는 메시지가 표시됩니다.
- 3. Display Certificate Request to terminal(터미널에 인증서 요청 표시)의 경우 **yes(예**)를 입력하 고 출력을 Verisign으로 전송합니다.
- 4. 새 인증서를 제공하면 다음 명령을 입력합니다. crypto ca import verisign 인증서

설치된 인증서 보기

- 1. Configuration(컨피그레이션)을 클릭하고 Properties(속성)를 클릭합니다.
- 2. Certificate(**인증서**)를 확장하고 Manage **Certificates(인증서 관리)를 선택합니다**.신뢰 지점 인 증에 사용된 CA 인증서 및 타사 공급업체에서 발급한 ID 인증서가 Manage Certificates(인증 서 관리) 영역에 나타나야 합니다

Startup Wizard	Manage Certificates					
AAA Setup	Manage the Certifical	es associate	d with trustpoints.			
Anti-Spooting						
- Auto Update	Subject	Type	Trustpoint	Status	Usage	Add
	VeriSign Trial	CA	my.verisign.tru	Available	General Purpo	
E Certificate	webypn.cisco	Identity	my.verisign.tru	Available	General Purpo	Show Detail
Authentication						
						Refrech
Import Certificate						
Manage Certificates						Delete
Configuration						

ciscoasa
ciscoasa(config)# show crypto ca certificates
<pre>! Displays all certificates installed on the ASA. Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5ele30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure Server Test CA ou=Terms of use at https://www.verisign.com/cps/testca (c)05 ou=For Test Purposes Only. No assurances. o=VeriSign Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of use at www.verisign.com/cps/testca (c)05 ou=TSWEB o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP</pre>
AIA: URL: http://ocsp.verisign.com CRL Distribution Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start date: 00:00:00 UTC Jul 19 2007 end date: 23:59:59 UTC



웹 브라우저를 사용하여 WebVPN에 설치된 인증서 확인

WebVPN에서 새 인증서를 사용하는지 확인하려면 다음 단계를 완료하십시오.

- 1. 웹 브라우저를 통해 WebVPN 인터페이스에 연결합니다. 인증서 요청에 사용한 FQDN(예: https://webvpn.cisco.com)과 함께 https://을 사용합니다.이러한 보안 경고 중 하나를 수신하는 경우 해당 경고에 해당하는 절차를 수행합니다. **보안 인증서 이름이 잘못되었거나 사이트 이름** 과 일치하지 않습니다. ASA의 WebVPN 인터페이스에 연결하기 위해 올바른 FQDN/CN을 사 용했는지 확인합니다. ID 인증서를 요청할 때 정의한 FQDN/CN을 사용해야 합니다. 인증서 FQDN/CN을 확인하기 위해 show crypto ca certificates trustpointname 명령을 사용할 수 있습 니다. 신뢰할 수 없도록 선택한 회사에서 보안 인증서를 발급했습니다.웹 브라우저에 타사 공 급업체 루트 인증서를 설치하려면 다음 단계를 완료하십시오.Security Alert(보안 경고) 대화 상자에서 View Certificate(인증서 보기)를 클릭합니다.Certificate(인증서) 대화 상자에서 Certificate Path(인증서 경로) 탭을 클릭합니다.발급된 ID 인증서 위에 있는 CA 인증서를 선택 하고 View Certificate(인증서 보기)를 클릭합니다.Install Certificate를 클릭합니다.Certificate Install Wizard(인증서 설치 마법사) 대화 상자에서 Next(**다음**)를 클릭합니다. **인증서 유형**에 따 라 인증서 저장소를 자동으로 선택 라디오 버튼을 선택하고 다음을 클릭한 다음 마침을 클릭 합니다.인증서 설치 확인 프롬프트를 받으면 예를 클릭합니다.가져오기 작업이 성공 프롬프트 에서 확인을 클릭하고 예를 클릭합니다. 참고: 이 예에서는 Verisign Trial Certificate를 사용하 므로 사용자가 연결할 때 확인 오류를 방지하려면 Verisign Trial CA Root Certificate를 설치해 야 합니다.
- 2. WebVPN 로그인 페이지의 오른쪽 아래 모서리에 나타나는 잠금 아이콘을 두 번 클릭합니다 .설치된 인증서 정보가 나타나야 합니다.
- 3. 콘텐츠를 검토하여 타사 공급업체 인증서와 일치하는지 확인합니다

Certificate		<u>?</u> ×
General Details Certification Path		
Certificate Information		
This certificate is intended for the following purpose(s):		
•Ensures ti	ne identity of a remote computer	
* Defer to the ce	rtification authority's statement for details	
	a chicación additioncy siscacement for decails.	- 11
Issued to	: webvpn.cisco.com	
Issued by	: VeriSign Trial Secure Server Test CA	
Valid from 8/14/2007 to 8/29/2007		
	Install Certificate Issuer Stateme	nt
	0	к

SSL 인증서 갱신 단계

SSL 인증서를 갱신하려면 다음 단계를 완료합니다.

- 1. 갱신해야 하는 신뢰 지점을 선택합니다.
- 2. 등록을 **선택합니다**.다음 메시지가 나타납니다.*다시 등록되면 현재 인증서가 새 인증서로 교체* 됩니다. 계속하시겠습니까?
- 3. 예를 선택합니다.그러면 새 CSR이 생성됩니다.
- 4. CA에 CSR을 보낸 다음 새 ID 인증서를 가져오면 가져옵니다.
- 5. 외부 인터페이스에 신뢰 지점을 제거하고 다시 적용합니다.

명령

ASA에서는 명령줄에서 여러 show 명령을 사용하여 인증서의 상태를 확인할 수 있습니다.

- show crypto ca trustpoint 구성된 신뢰 지점을 표시합니다.
- show crypto ca certificate 시스템에 설치된 모든 인증서를 표시합니다.

- show crypto ca crls 캐시된 CRL(certificate revocation list)을 표시합니다.
- show crypto key mypubkey rsa 생성된 모든 암호화 키 쌍을 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

다음과 같은 몇 가지 오류가 발생할 수 있습니다.

- % 경고: CA 인증서를 찾을 수 없습니다. 가져온 인증서를 사용할 수 없습니다.정보: 인증서를 가져왔습니다.CA 인증서가 올바르게 인증되지 않았습니다. CA 인증서가 설치되었는지 확인하 려면 show crypto ca certificate trustpointname 명령을 사용합니다. CA 인증서로 시작하는 행 을 찾습니다. CA 인증서가 설치된 경우 올바른 신뢰 지점을 참조하는지 확인합니다.
- 오류: 가져온 인증서를 구문 분석하거나 확인하지 못했습니다.이 오류는 ID 인증서를 설치하고 관련 신뢰 지점으로 인증된 올바른 중간 또는 루트 CA 인증서가 없을 때 발생할 수 있습니다. 올바른 중간 또는 루트 CA 인증서를 제거하고 다시 인증해야 합니다. 올바른 CA 인증서를 받았 는지 확인하려면 타사 공급업체에 문의하십시오.
- 인증서에 범용 공개 키가 없습니다.이 오류는 ID 인증서를 잘못된 신뢰 지점에 설치하려고 할 때 발생할 수 있습니다. 잘못된 ID 인증서를 설치하려고 시도했거나, 신뢰 지점과 연결된 키 쌍 이 ID 인증서에 포함된 공개 키와 일치하지 않습니다. ID 인증서를 올바른 신뢰 지점에 설치했 는지 확인하려면 show crypto ca certificates trustpointname 명령을 사용합니다. 연결된 신뢰 지점을 나타내는 줄을 찾습니다. 잘못된 신뢰 지점이 나열되면 이 문서에 설명된 절차를 사용하 여 적절한 신뢰 지점을 제거하고 다시 설치합니다. 또한 CSR이 생성된 이후 키 쌍이 변경되지 않았는지 확인합니다.
- 오류 메시지: %PIXIASA-3-717023 SSL이 신뢰 지점[신뢰 지점 이름]에 대한 장치 인증서를 설 정하지 못했습니다.이 메시지는 SSL 연결을 인증하기 위해 지정된 신뢰 지점에 대한 디바이스 인증서를 설정할 때 오류가 발생할 경우 표시됩니다. SSL 연결이 설정되면 사용할 디바이스 인 증서를 설정하려고 시도합니다. 오류가 발생하면 디바이스 인증서를 로드하는 데 사용해야 하 는 구성된 신뢰 지점 및 실패 이유를 포함하는 오류 메시지가 기록됩니다.trustpoint name -SSL에서 디바이스 인증서를 설정하지 못한 신뢰 지점의 이름입니다.권장 작업: 실패 이유로 표 시된 문제를 해결합니다.지정된 신뢰 지점이 등록되어 있고 디바이스 인증서가 있는지 확인합 니다.디바이스 인증서가 유효한지 확인합니다.필요한 경우 신뢰 지점을 다시 등록합니다.

관련 정보

- ASA에서 ASDM을 사용하여 Microsoft Windows CA에서 디지털 인증서를 얻는 방법
- <u>보안 제품 필드 알림</u>
- <u>RFC(Request for Comments)</u>
- <u>기술 지원 및 문서 Cisco Systems</u>